STUDIA UNIVERSITATIS MOLDAVIAE, 2019, nr.2(122)
Seria "Științe exacte și economice" ISSN 1857-2073 ISSN online 2345-1033 p.38-47

CZU: 004.056

SECURITATEA INFORMAȚIEI VIS-À-VIS DE SECURITATEA INFORMAȚIONALĂ

Tudor BRAGARU, Valentin BRICEAG, Viorel MALCOCI, Valeriu GALAICU

Universitatea de Stat din Moldova

Precizați semnificația cuvintelor și veți izbăvi omenirea
de o parte considerabilă a derutărilor sale.
René Descartes

În prezent, la nivel internațional se vehiculează mai mulți termeni similari, cum ar fi securitatea informației, securitatea informațională și securitatea cibernetică. Dar pot oare aceste concepte să se substituie unul pe altul sau sunt diferite? Și la nivel național multă lume întâmpină dificultăți majore în ce privește înțelegerea și aplicarea corectă a acestor concepte, care, în funcție de context, uneori pot fi considerate ca sinonime, alteori pot fi diferite, inclusiv ca sarcini, funcții, impact, arie de acoperire etc. Lucrarea urmărește să aducă o mai bună înțelegere și conștientizare a terminologiei, fiind utilă pentru persoanele implicate în activități educaționale (elevi, studenți, profesori, doctoranzi), pentru cei angajați în activități informaționale și/sau de securitate a informației.

Cuvinte-cheie: *securitatea informației, securitate informațională, securitate cibernetică, securitatea sistemelor informaționale, securitatea TIC.*

THE INFORMATION SECURITY VIS-a-VIS INFORMATIONAL SECURITY

Nowadays, worldwide, there are a lot of similar terms, such as information security, informational security and cybersecurity. But could these terms be replaced by each other or are they different? Nationwide, many people encounter major difficulties in understanding and correctly applying these terms, which, depending on context, can be sometimes considered synonyms or can be different by meaning, tasks, functions, impact or coverage. The paper aims at leading to a better understanding and awareness of this terminology, being useful for a wide range of users with educational activities (pupils, students, teachers, PhD students) and/or people engaged in informational and/or information security activities.

Keywords: *information security, informational security, cybersecurity, information system security, ICT security.*

1. Actualitatea securității informației și a securității informaționale

Astăzi *securitatea informației* a devenit un subiect deosebit de actual, care persistă practic pe agenda tuturor conferințelor și forurilor de specialitate, totodată constituind obiectul mai multor programe, proiecte, strategii etc. Aceasta se datorează faptului că, pe de o parte, informația este estimată la nivelul celui de-al patrulea element vital, *după aer, apă și foc,* iar, pe de altă parte, că era informațională a adus schimbări profunde în evoluția riscurilor și a modului în care *instituțiile statului, organizațiile private, persoanele individuale și societatea în întregime* ar trebui să răspundă provocărilor și oportunităților create de revoluția tehnologică.

Simultan cu creșterea disponibilității dispozitivelor electronice, inclusiv a celor portabile și a accesului fără fir la Internet, cu dezvoltarea domeniului tehnologiilor informaționale și comunicațiilor electronice (TIC), cu extinderea ariei afacerilor electronice operaționale, a hiper-conectivității globale, a serviciilor de cloud-computing *(SaaS – Software as service, IaaS – Infrastructure as service, PaaS – Platform as service)*, cu creșterea numărului de IoT (*Internet of Things, inclusiv case inteligente – Smart Home*) conectate la Internet etc., cresc și amenințările la adresa securității informației, dependentă de infrastructura TIC la nivel de stat, corporații/organizații și persoane fizice. Iar ușurința în utilizare, costul scăzut, rapiditatea și asigurarea unui caracter anonim fac Internetul și Webul un mediu favorabil pentru diverse infracțiuni în domeniu.

Evoluția infrastructurilor TIC moderne distribuite și interconectate face amenințările de securitate tot mai variate și mai complexe. Ca urmare, astăzi de domeniul TIC depind comunicațiile zilnice, tranzacțiile bancare și sistemele de achitări reciproce; controlul și gestionarea funcționalităților caselor de locuit, clădirilor, oficiilor de lucru, a transportului (aerian, feroviar, naval); furnizarea de energie, apă, gaz, căldură; educația, cercetarea, comerțul, serviciile medicale etc. Iar automatizarea acestora mărește simțitor nu doar viteza proceselor, ci și amploarea riscurilor, impactul incidentelor informaționale, pierderile cauzate, cheltuielile impuse pentru menținerea nivelului acceptabil al securității informaționale.

Doar pentru ilustrare, în Figura 1 este prezentată dinamica daunelor financiare cauzate de crima cibernetică între anii 2001 și 2017. *Alte diverse statistici ce denotă actualitatea securității informației a se vedea pe*

pagina web statista.com, care oferă statistici, rapoarte, info-grafice și altele în cadrul a peste 600 de industrii din 50 de țări, cu peste 6 milioane de utilizatori lunar din 195 de țări ale lumii.

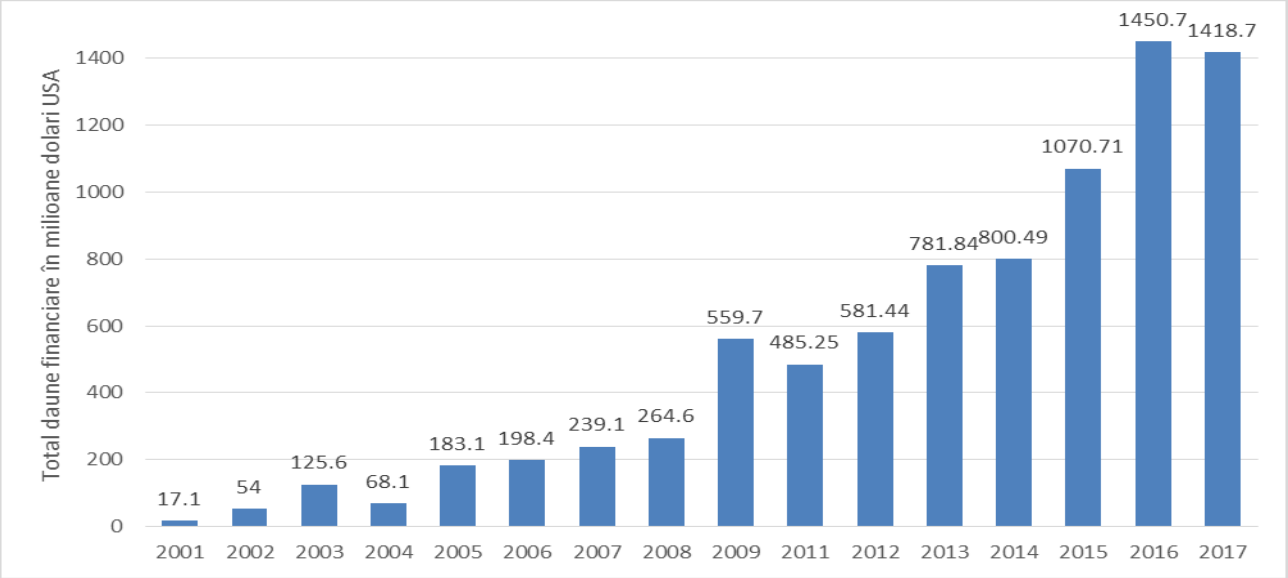

Fig.1. Dinamica daunelor financiare cauzate de crimele cibernetice între anii 2001 și 2017 [1].

Conform statisticilor, *criminalitatea informatică* rămâne a fi o *amenințare perpetuă* pentru interesele naționale și economice ale țărilor și corporațiilor. Iar securitatea informației *a devenit esențială atât pentru persoane fizice și juridice, cât și pentru societate și stat în întregime, ca componentă semnificativă a securității naționale și regionale*.

La nivel național nu există un consens în ceea ce privește terminologia domeniului securității informației, subdomeniile/componentele sale și cadrul de abordare. O problemă în acest sens este și lipsa unui cadru definitoriu clar stabilit în limba română cu traducerea polivalentă a termenului *information security* din limba engleză ca *securitatea informației* sau *securitatea informațională* sau altfel, ceea ce duce, adesea, la confuzii și dezorientări în abordarea și soluționarea problemelor de securitate. Totodată, din punct de vedere juridic, există mai multe legi și acte normative emise de instituțiile statului în care sunt definite noțiuni legate de domeniul TIC și, respectiv, de domeniul securității informaționale.

Scopul propus în prezenta lucrare este să aducem o mai bună înțelegere a terminologiei și a cadrului de abordare a *securității informației, securității informaționale, securității cibernetice* și a componentelor lor (*securitatea informatică, securitatea tehnologiei informației (IT), securitatea sistemelor informaționale (IS) etc.),* a legăturii dintre ele și cu alte domenii, cum ar fi *securitatea afacerii, securitatea întreprinderii, securitatea națională*. Doar cunoscând frontierele acestor domenii și conexiunile între ele pot fi rezolvate diversele probleme practice de securitate ce țin de context, domeniu, exigențe și reglementări.

2. Să înțelegem corect și să aplicăm adecvat cadrul conceptual și terminologic

Adesea, termenul *securitate informațională* este folosit (slab spus incorect) ca sinonim pentru termenul *securitatea informației,* în realitate acestea fiind două concepte *interdependente*, dar diferite ca arie de acoperire, amploare, obiective, sarcini, instrumente utilizate.

În lume, conceptul de **securitate a informației** este definit aproape în mod egal/identic de către majoritatea organizațiilor internaționale de standardizate. **Institutul Național de Standardizare și Tehnologie** (NIST) din SUA prin seria de standarde NIST SP-800 [2] se referă la necesitățile de securitate și confidențialitate a Departamentului de Stat al USA asupra *informației* și a sistemelor de procesare a informațiilor, în mare parte accentul fiind pus pe **securitatea informației în sistemele cibernetice**. Comitetul pentru securitatea datelor din industria cardurilor de plată prin standardul **PCI DSS** (*Payment Card Industry Data Security Standard)* stabilește cerințe de securitate aplicabile pentru toate componentele de sistem incluse sau conectate la *mediul de date* al deținătorilor de carduri bancare [3]. Organizația Internațională pentru Standardizare și Comisia Internațională pentru Electrotehnică (**ISO/IEC**) în familia de standarde ISO/IEC 27k [4] pune accentul pe

informație ca un bun fundamental al organizației, care trebuie protejat corespunzător, iar tehnologia informației și a comunicațiilor electronice este, de obicei, un element esențial în crearea, procesarea, stocarea, transmiterea, protecția și distrugerea informației. Totodată, vocabularul mondial de electrotehnică **Electropedia** [5] definește termenul de *securitate a informației* ca *protecția informațiilor împotriva divulgării, transferului, modificării sau distrugerii neautorizate*, indiferent de natura accidentală sau intenționată. **Uniunea Internațională a Telecomunicațiilor (ITU)** în privința securității informației face referință la seria de standarde NIST SP-800 și la familia de standarde ISO/IEC 27k. Cei de la ITU au creat, în baza ISO/IEC 27002, recomandările ITU-T X.1051 [6], care servesc ca *linii directoare pentru managementul securității informației în sistemele și serviciile de telecomunicații*. În esență, securitatea informației presupune *asigurarea protecției caracteristicilor fundamentale ale informațiilor: Confidențialitate, Integritate* și *Disponibilitate*, în literatura de specialitate referită ca triada CIA (Confidentiality, Integrity and Availability). Însă, în afară de protecția CIA, NIST, ISO, și alte organe de reglementare impun asigurarea și altor atribute adiționale bazate pe CIA, precum *dreptul de posesie a informației*, *autenticitatea informației* (asigurarea că un mesaj, o tranzacție sau un alt schimb de informații provin din sursa pe care se pretinde că este), *non-repudierea* (incapacitatea de negare a faptului emiterii informației și verificarea cu ușurință a emitentului), *fiabilitatea* (gradul de încredere). Totodată, acestea subliniază *diversitatea formelor de manifestare a informației*, *diversitatea dispozitivelor și tehnologiilor informaționale și comunicaționale* în procesele de stocare-prelucrare-transmitere etc.

Securitatea informațională, comparativ cu securitatea informației, reflectă o realitate sistemică mai complexă, înglobând în sine atât *securitatea informației, securitatea sistemelor informaționale (IS), securitatea informatică (a calculatoarelor, a rețelelor și dispozitivelor de rețea, a tehnologiei informației (IT), adesea referită ca securitate cibernetică/securitatea informației în spațiul cibernetic, virtual, sau securitatea în Internet*), *protecția datelor cu caracter personal*, cât și *protecția drepturilor de autor, protecția drepturilor și libertăților omului în spațiul informațional, protecția spațiului informațional și a infrastructurii critice, protecția personalului care lucrează cu sistemele informaționale, protecția informației oficiale ale statului, inclusiv a informațiilor atribuite la secret de stat și a celor cu accesibilitate limitată, protecția spațiului informațional de impactul dezinformării* etc.

Conceptul de securitate informațională este aplicabil la nivelul *persoanei, statului și al societății în întregime*, curent definită ca Societate Informațională bazată pe Cunoaștere. ***„Securitate informațională*** *– stare de protecție a resurselor informaționale, precum și a persoanei, a societății și a statului în spațiul informațional...* ***Spațiu informațional*** *– mediu de activitate asociat cu formarea, crearea, transformarea, transmiterea, difuzarea, utilizarea și stocarea informațiilor, care produce efecte la nivel de conștiință individuală și/sau socială, de infrastructură informațională și de informație"* [7]. *„Prin sintagma „securitate informațională" se are în vedere protecția persoanei, societății și a statului, a drepturilor și intereselor acestora în mediul informațional"* de amenințările asupra caracteristicilor fundamentale ale informației [8].

Securitatea informațională implică *tipul activului protejat* ca parte componentă a unui sistem informațional și al *activităților care contracarează provocarea daunelor obiectului dat*. În calitate de *obiect* fiind considerat *orice bun, sistem, informație, resursă umană, proces* ce are valoare pentru persoană, organizație, societate și stat. În acest caz, conceptul de *securitate informațională* se referă la *protecția de amenințările informaționale, când însuși obiectul protecției poate fi parte componentă sau proprietate a persoanei, a organizației, a unui sistem, a unei infrastructuri, a societății sau a statului în întregime*. De exemplu: *protecția datelor personale ale utilizatorului* vis-à-vis de *protecția informațională a persoanei* (de spam, reclamă nesolicitată etc.); *protecția informației oficiale a statului* vis-à-vis de *protecția spațiului informațional al statului* etc.

În general, conceptul de securitate informațională este preluat ca model de asigurare a securității resurselor informaționale la nivel de stat. Exemple în acest sens pot servi: **Concepția securității informaționale a Republicii Moldova** [9], în care asigurarea securității informaționale este definită ca stare de protecție a resurselor informaționale, precum și a persoanei, societății și statului, în spațiul informațional, iar spațiul informațional, la rândul său, este divizat în digital, cibernetic și mediatic; **Doctrina securității informaționale a Federației Ruse** [10], prin care se garantează protecția împotriva amenințărilor informaționale interne și externe în scopul asigurării drepturilor constituționale și libertăților oamenilor și ale cetățenilor.

Sintetizând, conceptul de *securitate informațională se referă la orice informații, IT sau non-IT (cărți, rapoarte, documente etc.), pe orice suporturi tradiționale (hârtie, pânză etc.) sau media electronice (bandă magnetică, CD etc.), sub orice formă (text, grafică, audio, video), comunicate în mod tradițional (scris, oral, poșta obișnuită) sau electronic (e-mail, chat, telefonie mobilă).*

La nivel de stat, în țara noastră există cadrul normativ general de acces la informațiile oficiale stabilit prin *Legea privind accesul la informație* [8], unde este definit termenul *informații oficiale*, care sunt considerate toate informațiile aflate în posesia și la dispoziția furnizorilor de informații, iar politica statului în domeniul accesării informațiilor oficiale presupune că oricine are dreptul de a le prelucra în condițiile prevăzute de această lege. Totodată, este definită o categorie de informații oficiale care posedă accesibilitate limitată, din care fac parte așa informații ca *informațiile cu caracter personal, informațiile atribuite la secretul de stat* ș.a.

Or, domeniul securității informației se referă *la orice acțiune, care implică asigurarea securității informațiilor* sau a *sistemelor informatice sau non-informatice care prelucrează informații,* inclusiv *componenta umană, componenta de infrastructură, componenta de suport pentru procesare-transportare-comunicare*, inclusiv în rețele, Internet, la distanță, online etc. Evident, *fiecare dintre aceste componente exercită impact asupra securității informației și constituie domeniu aparte, fiecare cu metodele și soluțiile sale*. De exemplu, asigurarea triadei CIA, autenticității și non-repudierii unui document pe suport de hârtie oarecum diferă de un document electronic, aplicarea semnăturii olografe diferă tehnologic de aplicarea semnăturii electronice, modul de păstrare la fel este diferit etc.

În concluzie, **securitatea informațională**, în mod general, poate fi definită ca *stare a spațiului informațional, care asigură nevoile informaționale ale subiecților în relațiile informaționale, securitatea informațiilor și protecția subiecților relațiilor informaționale de influențe negative*. Iar *spațiul informațional* poate fi definit drept *mediu de activitate a subiecților preocupați de crearea, transformarea și consumul de informații*. Astfel, conceptul *„securitate informațională" este unul acoperitor, care include nu doar securitatea informațiilor, ci și protecția mediului obiectului (statului, organizației, persoanei) de impactul informațiilor negative sau de destabilizarea unor componente ale sistemului/obiectului respectiv*. Rezumând, securitatea informațională poate fi definită ca *protejarea persoanei, organizației, societății și statului în spațiul informațional, a drepturilor și intereselor acestora față de (1) acces, (2) utilizare, (3) divulgare, (4) modificare, (5) dislocare sau (6) distrugeri neautorizate ale atributelor informației, ale IS, TIC și infrastructurilor de procesare, depozitare, acces și transport al informațiilor, **inclusiv** mass-media, în scopul asigurării intimității persoanei, continuității afacerii, suveranității statului, diminuării pierderilor, dezinformării, **inclusiv** prevenirii scurgerii de date, spionaj*.

Securitatea cibernetică este un alt concept vehiculat la nivel internațional cu sens apropiat de securitatea informației și securitatea informațională. Dacă *securitatea informațională* se referă la *orice securitate care implică securitatea informațiilor sau sistemelor informaționale,* atunci *securitatea cibernetică* are sensul de „*...orice securitate legată de spațiul cibernetic, care este un mediu complex ce apare în procesul de interacțiune a persoanelor, a software-ului și a serviciilor internet furnizate prin dispozitive tehnologice sau rețele integrate*" (adaptat conform ISO/IEC 27032).

În afară de protecția CIA, securitatea cibernetică include securitatea informatică/IT, se concentrează pe protecția datelor, programelor și infrastructurilor critice: rețele Intranet-Extranet-Internet, computere, servere și alte elemente ale infrastructurii IT comune și modul în care acestea pot fi utilizate împreună, pentru a spori beneficiile unei afaceri, organizații sau stat, având în vedere nu doar măsurile protective, ci și proactive. În linii mari, conceptul de securitate cibernetică din ISO/IEC 27032 corespunde definiției securității informației conform ISO/IEC 27000, care se referă la organizații social-economice.

În Republica Moldova, securitatea cibernetică, în esența sa, este parte componentă a concepției securității informaționale care, la rândul său, este parte componentă a strategiei naționale de apărare, definită în documentele strategice privind securitatea națională [13], accentuând nu doar componenta sa defensivă, de apărare, ci și pe cea ofensivă, orientată spre combaterea unor dificultăți, lichidarea unor situații neconvenabile.

Securitatea cibernetică este abordată la nivel de cadru comunitar în majoritatea țărilor Uniunii Europene (UE) în baza directivelor europene și a recomandărilor **ENISA** *(European Union Agency for Network and Information Security)*. Din analiza efectuată în Strategia națională de securitate cibernetică [13] reiese că în 2012 majoritatea țărilor UE deja aveau în lucru cadrul normativ de securitate cibernetică. În România, prin *Legea privind securitatea cibernetică a României,* sunt puse în aplicare măsuri complexe de organizare și desfășurare a activităților din domeniul securității cibernetice și de asigurare a protejării drepturilor și libertăților fundamentale ale cetățenilor în spațiul cibernetic.

Veriga principală care leagă între ele conceptele de securitate examinate, precum și cu alte concepte conexe, cum ar fi *continuitatea afacerii, securitatea informației întreprinderii,* este **managementul riscurilor** (Fig.2). Standardul ISO 31000 se referă la toate riscurile în general, inclusiv la partea de securitate a informației.

Iar asigurarea caracteristicilor fundamentale ale informației, care stă la baza conceptelor înrudite de securitate a informației și abordarea procesuală comună bazată pe analiza riscurilor, face posibilă *integrarea conceptelor și sistemelor adiacente de management al securității informației, al calității, al continuității afacerii, al securității cibernetice și al securității informaționale.*

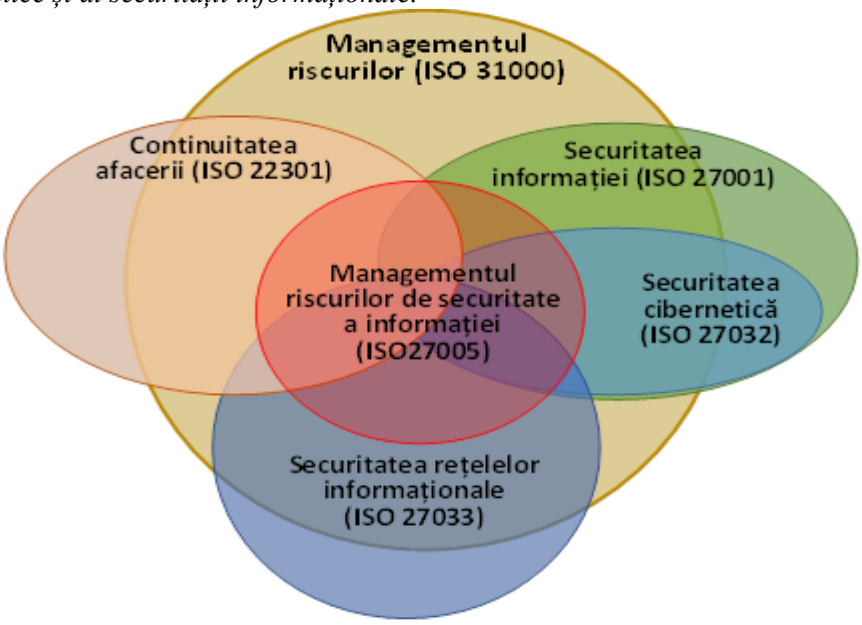

Fig.2. Legătura dintre diferite tipuri de securitate: toate intră sub umbrela managementului riscurilor *(adaptată după* [14]*).*

Prin analogie cu diagrama din Figura 2, integrarea conceptelor de securitate în cadrul unei singure pseudo-diagrame de tip Venn (Fig.3) permite înțelegerea relațiilor dintre ele, inclusiv coraportul lor. Securitatea informațională constituie un mega-concept de cel mai înalt nivel, care include în sine pe toate celelalte tipuri de securitate a informației ca componente interdependente. La rândul său, în sfera securității informațiilor este inclusă securitatea cibernetică *(în Internet)*, securitatea mediatică și așa mai departe până la cel mai de jos nivel, ce include suporturile de informații, codurile utilizate etc.

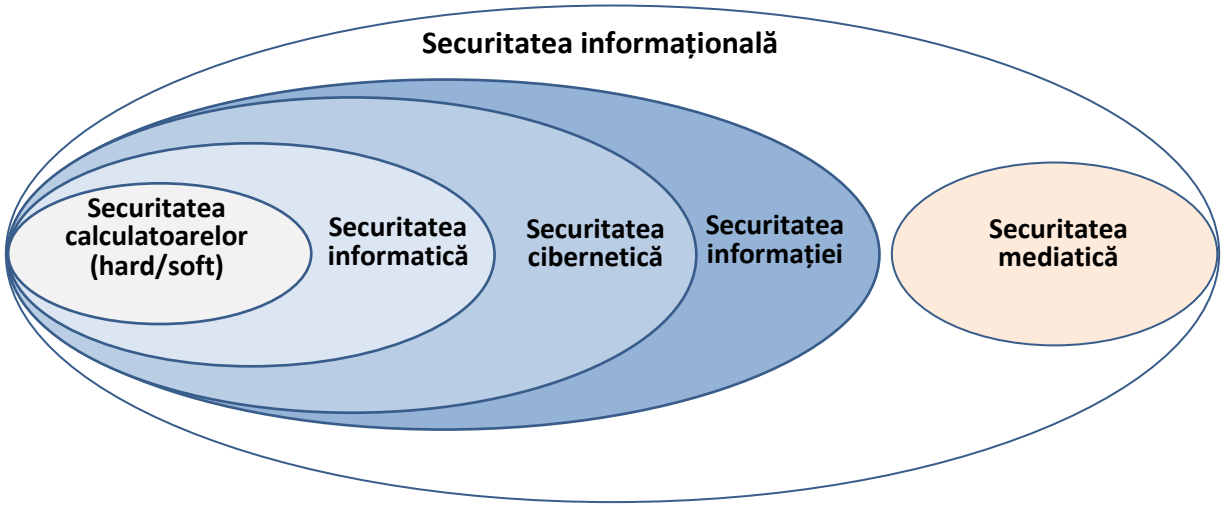

Fig.3. Ierarhia diferitelor tipuri de securitate și volumul lor sugestiv.

Totodată, cele prezentate în Figura 3 sugerează și *strategia de abordare a securității informației în adâncime*, pe straturi, fiecare dintre ele cu problemele, metodele, soluțiile și mecanismele sale specifice de protecție. Apărarea în adâncime presupune plasarea valorilor cât mai în interiorul ariei de protecție și protecția cu mai multe bariere concentrice. În acest context este de menționat că *compromiterea securității la cel mai de jos nivel duce la compromiterea securității la toate nivelurile, până la cel mai de sus nivel, și invers*.

Unii cercetători practicieni (de ex., *Dejan Kosutic)* afirmă că securitatea cibernetică a corporației reprezintă cca 95% din securitatea informațiilor; diferența dintre ele este că securitatea informației include și informații non-digitale (de exemplu, pe suport de hârtie), în timp ce securitatea cibernetică se concentrează doar pe informații în formă digitală. Totodată, mulți afirmă despre raportul de 50:50 dintre securitatea informației și securitatea informatică/IT. Considerăm că ar trebui aplicat *principiul universal Pareto (80/20),* unde securitatea informatică să reprezinte cca 80% din securitatea informațiilor, celelalte 20% acoperind securitatea fizică, gestionarea resurselor umane, protecția juridică, organizarea, procesele. Unul dintre temeiurile acestei teze constă în utilizarea în masă a TIC, în marea lor diversitate și complexitate, inclusiv a măsurilor de securitate, pe de o parte, și a vulnerabilităților cauzate de factorul uman, pe de altă parte. **Automatizarea, intelectualizarea măsurilor de securitate ar diminua simțitor influența factorului uman**. De exemplu, *amenințările în adresa accesibilității/disponibilității,* considerate dintre cele mai frecvente și mai periculoase *(conform estimărilor experților, până la 65-80% din pierderi),* sunt cauzate de erori intenționate sau accidentale ale utilizatorilor interni, ale administratorilor de sistem, ale operatorilor și altor persoane ce deservesc IS/IT, de nivelul relativ scăzut al culturii lor informaționale și/sau de complexitatea protecției. Ca urmare, o eventuală soluție de diminuare cardinală a acestor pierderi ar putea fi obținută din contul minimizării influenței factorului uman asupra securității prin automatizarea, intelectualizarea maximală a gestionării securității informaționale.

3. Securitatea informației în practică

Dar cum arată securitatea informației în practică? Problema e că securitatea informației include o gamă largă de domenii conexe, printre care *gestionarea riscurilor și gestionarea incidentelor informaționale, arhitectura și modelele securității calculatoarelor/sistemelor de operare, a bazelor de date, a sistemelor și aplicațiilor informaționale, securitatea infrastructurii programo-tehnice bazate pe rețele informaționale și de telecomunicații, inclusiv cu arhitectură deschisă OSI (Open System Interconnection, Internetul modern), securitatea fizică și securitatea de mediu, securitatea afacerii, securitatea operațională, securitatea personalului implicat* etc.

Un program complet de securitate cuprinde mai multe elemente interdependente și corelate (Fig.4).

Fig.4. Elementele unui program complet de securitate (*adaptată după* [15]).

Modelul programului de securitate are straturi diferite, cu diferite tipuri de obiective care trebuie realizate la intervale diferite de timp. Cele prezentate în Figura 4 sugerează *trei orizonturi ale managementului securității*

informației, redate prin trei cercuri concentrice, pornind de la *planificarea/managementul strategic,* la *planificarea/managementul tactic* către *planificarea/managementul operațional*.

Obiectivele pot fi zilnice (operaționale), pe termen mediu (tactic) și pe termen lung (strategice). Obiectivele operaționale ale securității informației sunt legate de productivitatea și implementarea sarcinilor curente, care asigură funcționarea companiei într-un mod previzibil. Obiectivele pe termen mediu și pe termen lung în domeniul securității informației sunt aliniate la obiectivele tactice/strategice ale organizației.

În centrul programului se află activele informaționale valoroase ale companiei, care trebuie protejate conform cerințelor legislative și de reglementare, modelului sistemului de management, politicii de securitate, infrastructurii etc. (cercul extern). Activele trebuie protejate atât la nivel fizic, cât și la nivel logic, în funcție de riscurile, amenințările și vulnerabilitățile specifice contextului organizației.

Cerințele de securitate, cerințele față de managementul securității informației, investigațiile incidentelor, auditul etc. sunt reglementate de o multitudine de standarde ISO/IEC, NIST, ISACA, ITU, OWASP *(Open web application security project).* Toate acestea și alte organizații mondiale preocupate de securitate au emis sumar peste 300 de standarde cu o multitudine de măsuri, proceduri, bune practici *(în total peste 3500!)*, care sunt astăzi în vigoare, sunt sistematic revizuite, îmbunătățite și reeditate.

Dacă ne gândim la multitudinea elementelor programului complet de securitate, la multitudinea de standarde, modele, măsuri, practici, proceduri de securitate etc., *lucrurile par a fi destul de complicate*. Într-adevăr, ca urmare a utilizării pe larg a Internetului și a conectivității globale, securitatea informației a devenit o preocupare globală, care nu se poate limita la frontierele unei firme/organizații/stat sau ale unui sistem izolat. Securitatea informației niciodată nu se rezumă la o singură măsură de securitate, efectuată o singură dată, impunând o mare diversitate de măsuri sistematic repetate, inclusiv măsuri noi ca răspuns la noile amenințări. Chiar dacă cea mai mare parte a informației este procesată în mod electronic, securitatea informației se referă nu doar la IS/IT, ci implică și diverse aspecte organizaționale, educaționale, legale și de personal.

Problema pare a fi destul de dificilă, dar nu și imposibil de soluționat. Deoarece pentru abordarea acestei probleme complexe deja există cadre metodologice prestabilite *(frameworks, modele)* sub forma unor standarde, precum familia ISO/IEC 27k, bune practici ITIL/ITSM *(familia de standarde ISO-20000),* seria publicațiilor speciale NIST *(SP 800, SP 500 etc.)*, PCI DSS, recomandări GDPR, CoBIT *(de la ISACA)* și altele. Întrebarea de bază este: Care ar fi cadrul potrivit unui caz concret? Evident, managementul securității informaționale sau a informației, soluțiile, costurile, implicațiile pentru diferite niveluri *(e.g. individual, firmă, stat, societate)* și diferite domenii de activitate *(e.g. servicii bancare, medicină)* va fi diferit, deoarece sunt diferite contextele, exigențele, produsele utilizate, personalul implicat etc.

În opinia noastră, cei mai importanți jucători pe piața securității sunt doi: ISO și NIST.

Familia/seria de standarde ISO/IEC- 27k (Fig.5) are la origine ISO/IEC BS7799 republicat în 2000 ca ISO/IEC 17799, republicat în 2005 ca **ISO/IEC- 27001.** Astăzi familia de standarde ISO/IEC 27k cuprinde peste 60 de standarde, 50 dintre care deja sunt publicate, multe dintre ele continuu reeditate/îmbunătățite, astfel că unele dintre ele au ajuns la ediția a 5-a. Este de menționat că familia ISO/IEC 27k *integrează cele mai bune practici și realizări ale standardelor anterioare din domeniul securității informației, astăzi fiind considerat cel mai potrivit cadru general de abordare a securității informatei.*

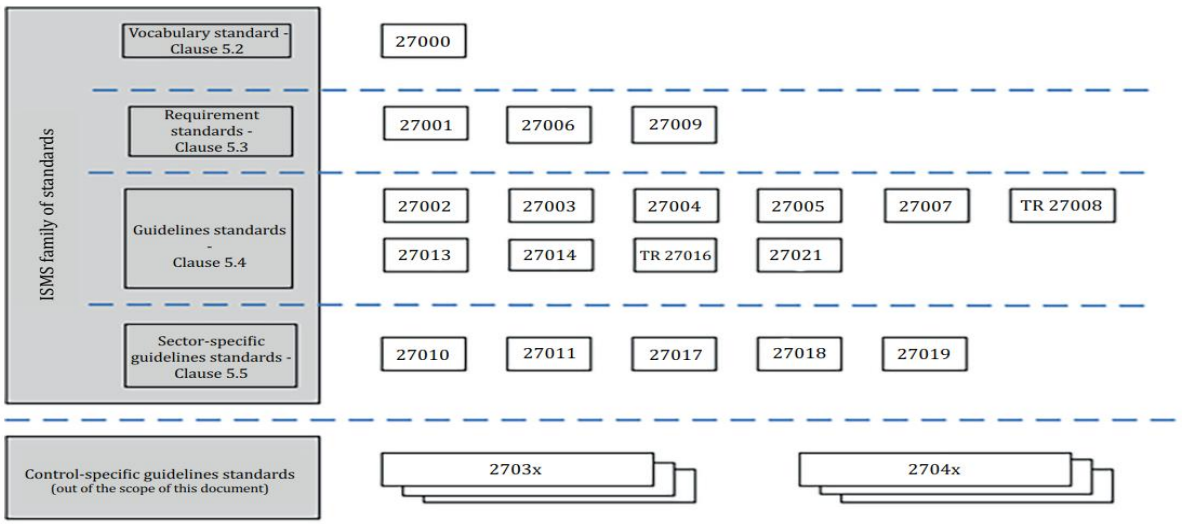

Fig.5. Cele mai populare standarde ale seriei ISO 27k și relațiile dintre ele (*reluată din ISO 27000:2018*).

Un alt jucător important pe piața **securității este NIST** (de la *National Institute of Standards and Technology, SUA.),* care dezvoltă și menține o vastă colecție de standarde, îndrumări, recomandări și cercetări privind securitatea informației, securitatea informatică, securitatea informațională. Una dintre subdiviziunile NIST – *Computer Security Resource Center (CSRC),* este preocupată de trei direcții principale:

- *Gestiunea securității informațiilor;*
- *Aspectele tehnice ale securității informațiilor;*
- *Protecția criptografică a informațiilor.*

Toate publicațiile CSRC pot fi văzute la adresa *http://csrc.nist.gov/publications*.

Seriile de publicații tehnice speciale (SP) includ instrucțiuni, specificații tehnice, recomandări și materiale de referință, grupate în câteva sub-serii:

- Seria publicațiilor speciale SP 800 *(https://www.nist.gov/itl/nist-special-publication-800-series-general-information)* cuprinde linii directoare, recomandări, specificații tehnice dezvoltate pentru a aborda și sprijini nevoile de securitate și confidențialitate a informațiilor și sistemelor informaționale ale guvernului SUA, dar ele sunt publice și pot fi aplicate și altor sistemelor naționale de securitate.
- Seria publicațiilor speciale SP 1800 *(https://www.nist.gov/itl/nist-special-publication-1800-series-general-information)*, prezintă *soluții* practice de securitate cibernetică în spațiul informatic/cibernetic, de uz informal pentru comunități de diferit nivel (e.g. companie, asociație, stat, societate).

Dar cel mai semnificativ progres NIST, care reflectă cu adevărat succesul modelului public-privat pentru abordarea provocărilor în domeniul securității cibernetice, este produsul său lansat în 2015 Cybersecurity Framework, în prezent utilizat de cca 30% din organizațiile din SUA și, conform Hartner, în 2020 acest număr este estimat să atingă 50%.

Cybersecurity Framework integrează standardele industriale și cele mai bune practici pentru a ajuta organizațiile să-și gestioneze riscurile de securitate cibernetică.

În concluzie, cel mai potrivit cadru general de management al securității informației ar fi ISO 27k în combinație cu măsuri, bune practici, recomandări concrete conform domeniilor specifice, conținute, de exemplu, în standardele și publicațiile speciale NIST, PCI DSS pentru sectorul bancar etc. ISO 27001 oferă o bază unică pentru construirea sistemului de securitate a informațiilor pentru orice fel de organizații, dar și flexibilitatea de a aplica doar acele controale prescrise de ISO 27002 sau NIST SPs, PCI DSS etc., care sunt cu adevărat necesare pentru protejarea domeniului concret de activitate, oferind o bună cale de a rezolva cu atenție orice problemă potențială și de a păstra informațiile în siguranță în mod continuu, cu participarea întregii companii, plecând de la managementul superior, consiliul executiv și terminând cu operatorii la locurile de muncă.

4. Schimbarea de paradigmă

Confruntată cu provocări de securitate informațională tot mai mari, societatea informațională bazată pe cunoaștere, ale cărei cele mai importante resurse ce trebuie organizate și valorificate corespunzător sunt resursele informaționale, caută să îmbunătățească gradul de conștientizare a *vulnerabilităților, amenințărilor de securitate* și *capacitatea de reacție* la atacuri premeditate; încearcă *să se adapteze transformărilor continue ale mediului de securitate* și *să folosească în avantajul său noile instrumente informaționale* pentru prevenirea și combaterea riscurilor tradiționale de securitate a informației, securitate informațională/cibernetică și a noilor amenințări. Însă, majoritatea soluțiilor, măsurilor, instrumentelor de securitate rămân astăzi suprapuse peste produsele/activele informatice, implementate deja după proiectarea/realizarea lor.

Începând cu anii 2005 se resimte **o nouă abordare** a acestui domeniu complex, prin *schimbarea accentelor de la o problemă preponderent tehnică și gestionată de IT – la una organizațională și gestionată de către managementul de vârf, de la orientarea pe sisteme – la orientarea pe procese, de la valoarea adăugată – la valoarea încorporată a securității*, toate acestea fiind resimțite în reglementările ISO, NIST, ITU, ISACA și ale altor organizații internaționale preocupare de securitatea informației la orice nivel.

Vechea abordare a securității informaționale, separată de înseși dispozitivele, sistemele, afacerile, activele informaționale, va fi, probabil, depășită în noua paradigmă. În noua abordare *securitatea este considerată ca parte integrantă indivizibilă a produselor informaționale, nu mai puțin importantă decât proprietățile funcționale*. Totodată, integrarea securității informației cu înseși produsele/tehnologiile informației ar trebui, în mod ideal, să facă securitatea transparentă, invizibilă în cadrul acestora.

Este de menționat și regândirea atitudinii față de securitate, ca set de reguli de comportament în mediul informațional, care ar permite păstrarea nivelului necesar de asigurare a principalelor caracteristici de securitate ale activelor informaționale, exprimate prin triada CIA *(Confidențialitate, Integritate, Disponibilitate/Accesibilitate)*. Noua paradigmă presupune trecerea de la metode pasive la metode proactive de preîntâmpinare a accesului ilicit, neautorizat la date, aplicații și alte resurse informaționale, de exemplu prin autentificarea multifactorială; de la divulgare, scurgere de date și informații confidențiale – la preîntâmpinarea acestora prin diminuarea influenței factorului uman și altele.

Una dinte soluțiile prioritare acceptabile în acest context ar fi *elaborarea unor noi strategii de integrare a securității încorporate în produse, creșterea ratei de eficiență prin automatizarea, intelectualizarea securității și a implementării mecanismelor de autentificare garantată* utilizând metode criptografice, cum ar fi semnătura electronică. Însă, acestea constituie un alt subiect complex, demn de examinare separată.

Referințe:

1. Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2017. Disponibil: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/
2. NIST Special Publication 800-series General Information. INFORMATION TECHNOLOGY LABORATORY. Nation Institute of Standards and Technologies: publicat 21.05.2018. Disponibil: https://www.nist.gov/itl/nist-special-publication-800-series-general-information
3. Payment Card Industry 3-D Secure (PCI 3DS). Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server. Security Standards Council: publicat octombrie 2017. Disponibil: Site. https://www.pcisecuritystandards.org/documents/PCI-3DS-Core-Security-Standard-v1.pdf?agreement=true&time=1553409032809
4. Information technology — Security techniques — Information security management systems — Overview and vocabulary. International Organization for Standardization. ISO/IEC 27000:2018, ediția V: publicat februarie 2018. Disponibil: http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
5. The World's Online Electrotechnical Vocabulary. Area: 721: Telegraphy, facsimile and data communication. International Electrotechnical Commission (UIT) (IEV ref. 721-08-57): publicat noiembrie 1991. Disponibil: http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=721-08-57
6. X.1051: Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations. International Telecomunication Unit (ITU): publicat 21.11.2016. Disponibil: https://www.itu.int/rec/T-REC-X.1051-201604-I/en
7. Legea privind Securitatea Cibernetica a României, versiunea finală, publicată la 04.04.2016. Disponibil: https://www.comunicatii.gov.ro/legea-privind-securitatea-cibernetica-a-romaniei-versiunea-finala/
8. MORARU, S. *Securitatea Națională a Republicii Moldova în contextul democratizării societății: aspecte politico-informaționale* / Cu titlu de manuscris. Chișinău, 2015.
9. Legea privind Concepția Securității Informaționale a Republicii Moldova, nr.299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr.48-57, art.122.
10. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации №646, от 5 декабря 2016 г. Disponibil: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html
11. Legea privind accesul la informație, nr.982 din 11.05.2000. În: *Monitorul Oficial al Republicii Moldova*, 2000, nr.88-90, art.664.
12. Hotărârea Parlamentului pentru aprobarea Strategiei naționale de apărare și a Planului de acțiuni privind implementarea Strategiei naționale de apărare pentru anii 2018–2022, nr.134 din 19.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr.285-294, art.441.
13. National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace. European Network and Information Security Agency (ENISA): Mai 2012. Disponibil: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
14. Dejan Kosutic. ISO 31000 and ISO 27001 – How are they related?
15. CISSP. Руководство для подготовки к экзамену. Ediția V. Disponibil: http://dorlov.blogspot.com/2011/05/issp-cissp-all-in-one-exam-guide.html

Notă: *Toate resursele web au fost accesate la 6 martie 2019.*

Date despre autori:
Tudor BRĂGARU, dr. conf. univ., Universitatea de Stat din Moldova.
E-mail: theosnume@gmail.com
ORCID: 0000-0001-6356-2906

STUDIA UNIVERSITATIS MOLDAVIAE, 2019, nr.2(122)
Seria "Ştiinţe exacte şi economice" ISSN 1857-2073 ISSN online 2345-1033 p.38-47

Valentin BRICEAG, doctorand, Școala doctorală *Matematică şi Ştiinţa Informaţiei*, Universitatea de Stat din Moldova.
E-mail: valentinbriceag@gmail.com
ORCID: 0000-0002-3963-1278
Valeriu MALCOCI, doctorand, Școala doctorală *Matematică şi Ştiinţa Informaţiei*, Universitatea de Stat din Moldova.
E-mail: vioacropolis@gmail.com
ORCID: 0000-0003-1842-906X
Valeriu GALAICU, doctorand, Școala doctorală *Matematică şi Ştiinţa Informaţiei*, Universitatea de Stat din Moldova.
E-mail: valeriugalaicu@gmail.com
ORCID: 0000-0002-0685-3536

Prezentat la 04.04.2019